“Київський фаховий коледж зв’язку”

Циклова комісія комп’ютерної та програмної інженерії

**ЗВІТ ПО ВИКОНАННЮ**

**ЛАБОРАТОРНОЇ РОБОТИ №10**

з дисципліни: «Операційні системи»

**Тема: «Зміна власників і прав доступу до файлів в Linux. Спеціальні каталоги та файли в Linux»**

Виконала студентка

групи РПЗ-13а

Балджі В.В.

Перевірив викладач

Сушанова В.С.

Київ 2024

**Тема: “Зміна власників і прав доступу до файлів в Linux. Спеціальні каталоги та файли в Linux”**

**Мета роботи:**

1. Отримання практичних навиків роботи з командною оболонкою Bash.
2. Знайомство з базовими діями при зміні власників файлів, .прав доступу до файлів
3. Знайомство з спеціальними каталогами та файлами в Linux.

**Матеріальне забезпечення занять:**

1. ЕОМ типу IBM PC.

2. ОС сімейства Windows та віртуальна машина Virtual Box (Oracle).

3. ОС GNU/Linux (будь-який дистрибутив).

4. Сайт мережевої академії Cisco netacad.com та його онлайн курси по Linux

**Завдання для попередньої підготовки:**

1. \*Прочитайте короткі теоретичні відомості до лабораторної роботи та зробіть невеличкий словник базових англійських термінів з питань призначення команд та їх параметрів.

|  |  |
| --- | --- |
| **Термін англійською** | **Термін українською** |
| initially created | спочатку створений |
| to accommodate | пристосуватися |
| presence | присутність |
| approach | підхід |
| contrary | навпаки |
| inherit | успадковувати |

1. Вивчіть матеріали онлайн-курсу “NDG Linux Essentials” (netacad.com):

* Chapter 17 - Ownership and Permissions
* Chapter 18 - Special Directories and Files

1. Пройдіть тестування у курсі NDG Linux Essentials за такими темами:

* Chapter 17 Exam
* Chapter 18 Exam

1. На базі розглянутого матеріалу дайте відповіді на наступні питання:
   1. Яке призначення команди id?

The id command can be useful for verifying which user account you are using and which groups you have available to use. By viewing the output of this command, you can see the user's identity information expressed both as a number and as a name. The output of the id command displays the UID and user account name of the current user followed by the GID and group name of the primary group and the GIDs and group names of all group memberships.

* 1. Як переглянути які права доступу має власник файлу?

The ownership of all files and subdirectories within the current directory can be listed using the ls -la command.

* 1. \*Як змінити власника групи?

To change the group owner of an existing file the chgrp command can be used.

* 1. \*Як можна переглянути у терміналі який тип поточного файлу? Наведіть приклади для різних типів файлів.

You can use the file command in the terminal.

Example 1

echo “This is a text file” > file.txt

file file.txt

Example 2

file1 /usr/bin/bash

* 1. \*\*Для чого використовуються дозволи Setuid та Setgid?

When the setuid permission is set on an executable binary file (a program) the binary file is run as the owner of the file, not as the user who executed it. This permission is set on a handful of system utilities so that they can be run by normal users, but executed with the permissions of root, providing access to system files that the normal user doesn't normally have access to.

The setgid permission is similar to setuid, but it makes use of the group owner permissions. There are two forms of setgid permissions: setgid on a file and setgid on a directory. The behavior of setgid depends on whether it is set on a file or directory.

* 1. \*\*Для чого в системі потрібен так званий “липкий біт” (Sticky Bit). Наведіть приклади коли цей дозвіл доцільно використовувати.

The *sticky bit* permission is used to prevent other users from deleting files that they do not own in a shared directory.

A good example of the use of sticky bit directories would be the /tmp and /var/tmp directories. These directories are designed as locations where any user can create a temporary file.

Because these directories are intended to be writable by all users, they are configured to use the sticky bit. Without this special permission, users would be able to delete any files in this directory, including those that belong to other users.

1. Підготувати в електронному вигляді початковий варіант звіту:

* Титульний аркуш, тема та мета роботи
* Словник термінів
* Відповіді на п.4.1-4.6 з завдань для попередньої підготовки

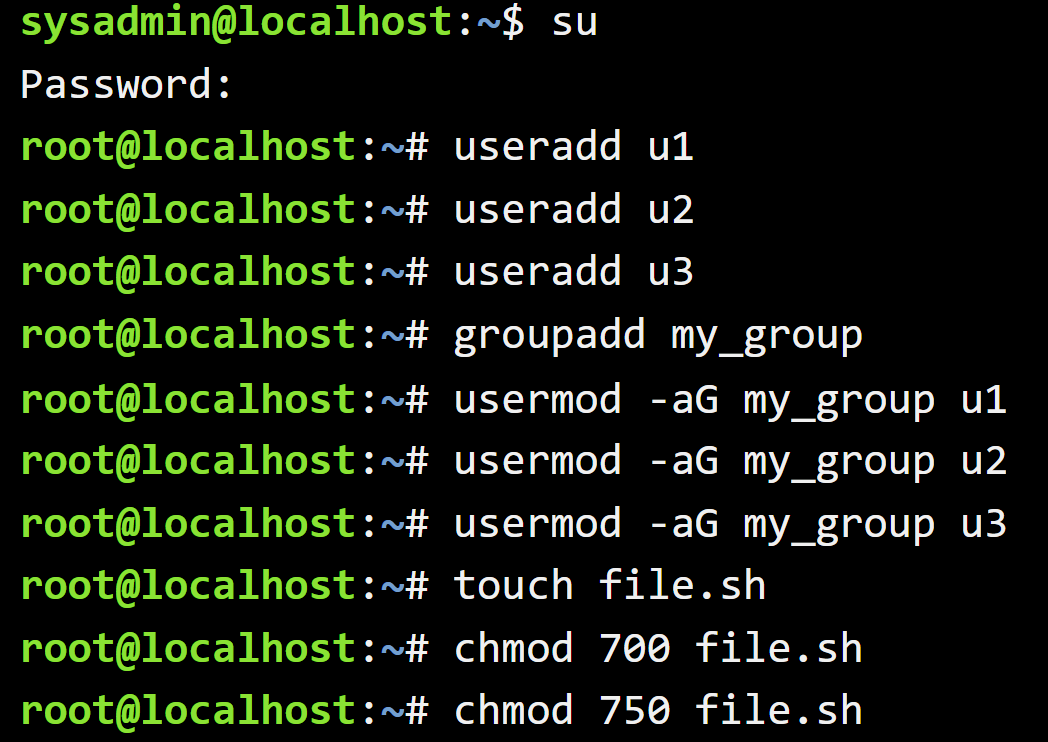
**Хід роботи:**

* 1. Початкова робота в CLI-режимі в Linux ОС сімейства Linux:
  2. Запустіть віртуальну машину VirtualBox, оберіть CentOS та запустіть її. Виконайте вхід в систему під користувачем: CentOS, пароль для входу: reverse ***(якщо виконуєте ЛР у 401 ауд.)*** та зпустіть термінал.
  3. Запустіть віртуальну машину Ubuntu\_PC ***(якщо виконуєте завдання ЛР через академію netacad)***
  4. Запустіть свою операційну систему сімейства Linux ***(якщо працюєте на власному ПК та її встановили)*** та запустіть термінал.
  5. Опрацюйте всі приклади команд, що представлені у лабораторних роботах курсу ***NDG Linux Essentials: Lab 17: Ownership and Permissions*** та ***Lab 18: Special Directories and Files.*** Створіть таблицю команд вивчених у п.2 ходу роботи у наступному вигляді:

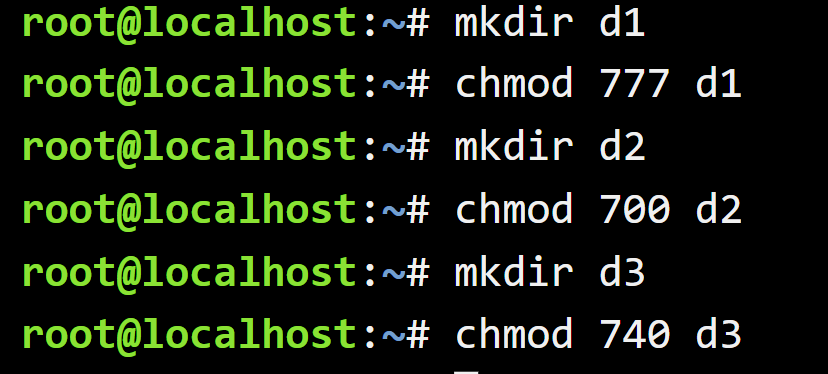
|  |  |
| --- | --- |
| Назва команди | Її призначення та функціональність |
| cd /tmp | Move to the /tmp directory. |
| mkdir priv-dir pub-dir | Use the mkdir command to create two directories called priv-dir and pub-dir. |
| touch priv-dir/priv-file  touch pub-dir/pub-file | Create two files, one file called priv-file in the priv-dir directory and another file called pub-file in the pub-dir directory. |
| ls -l priv-dir  ls -l pub-dir | Use this command to view the contents of the new directories. |
| ls -la | The ownership of all files and subdirectories within the current directory can be listed using the ls -la command. |
| ls -ld priv-dir/  chmod o-rx priv-dir/ | Use the ls -ld command to view permissions for the priv-dir directory, then use the chmod command to remove the others' permissions for read and execute. |
| ls -ld priv-dir/ | Finally, use the same ls command to verify the change in permissions |
| ls -ld pub-dir/  chmod o+w pub-dir/  ls -ld pub-dir/ | If you want to make a directory more public, then you can use the chmod command to add write permission for others. |
| ls -l priv-dir/priv-file  chmod g-rw,o-r priv-dir/priv-file  ls -l priv-dir/priv-file | Use the chmod command to remove any permission from the group and others on the priv-file. |
| ls -l pub-dir/pub-file  chmod a=rw pub-dir/pub-file  ls -l pub-dir/pub-file | Grant all users the same read and write permission for the pub-file. |
| echo "date" > test.sh | Create a test.sh file in the /tmp containing the content "date". |
| ./test.sh  ls -l test.sh | Attempt to execute the test.sh file; it should fail. View the permissions on the file to see why. |
| chmod u+x test.sh  ls -l test.sh  ./test.sh | Give yourself, the user owner, execute permission and then execute test.sh. |
| stat test.sh | Use the stat command to verify the octal value for the permissions (access) to test.sh. |
| chmod 775 test.sh  ls -l test.sh | Using octal notation, modify the permissions of the test.sh file, so everyone would be able to execute the file. |
| su - | Switch to the root user , so you will be able to execute both the chown and chgrp commands to change group ownerships to any group. |
| cd /tmp  ls -ld pub-dir  ls -l pub-dir/pub-file | Change back to the /tmp directory and list the details of the pub-dir, and then its contents. |
| chown root:root pub-dir  ls -ld pub-dir | Use the chown command to change the user and group owner of pub-dir to the root user and the root group. Then, view the details of the directory. |
| chown bin pub-dir/pub-file  ls -l pub-dir/pub-file | Use the chown command to change the user owner of the pub-file to the bin user. |
| ls -ld priv-dir  ls -l priv-dir/priv-file | View the details of the priv-dir and its contents. |
| ls -ld priv-dir  ls -l priv-dir/priv-file  chgrp -R users priv-dir  ls -ld priv-dir  ls -l priv-dir/priv-file | To change the group ownership of all of the files of a directory structure, use the recursive -R option to the chgrp command. Change the group owner of the priv-dir and priv-file to the users group recursively with the chgrp command and view the updated files. |
| ls -ld /tmp  ls -ld /var/tmp | Using the -d option for the ls command lists directory information; combined with the -l option it shows ownership and permissions for the directory files. List the details of the /tmp and /var/tmp directories. |
| ls -l /etc/shadow | View the permissions on the /etc/shadow file. |
| ls -l /usr/bin/passwd | View the permissions of the /usr/bin/passwd file. |
| ls -l /usr/bin/wall | View the permissions on the /usr/bin/wall command. |
| cd | Change to your home directory. |
| echo "data" > source | Create a file named source containing the text "data" by using redirection. |
| ls -li source | Using the -i option with the ls command prints the index number of the file. View the details and inode information of the source file. |
| ln source hardlink  ls -li source hardlink | Use the ln command to create a hard link. View the details and inode information of the source and new hard link file. |
| ln hardlink hardlinktwo  ls -li hardlink hardlinktwo source | Use the ln command to create another hard link to the source file. View the details and inode information of the source and new hard link files. |
| rm hardlinktwo  ls -li source hardlink | The rm command is used to remove files. Remove the last link that was created and list the source and hardlink files. |
| rm hardlink  ls -li source | Remove the hardlink file and list the source file details. |
| ln -s source softlink  ls -li source softlink | The -s option for the ln command creates a symbolic link instead of a hard link. Create a symbolic link to the source file and view the details of both files. |
| ln -s /proc crossdir  ls -l crossdir | Create a symbolic link to the /proc directory and display the link. |

**Примітка:** **Скріншоти** виконання команд в терміналі можна **не представляти**, достатньо **коротко описати команди в таблиці**.

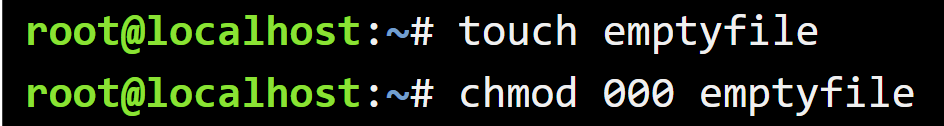
* 1. Виконайте наступні практичні завдання у терміналі наступні дії (продемонструвати скріншоти):
* створіть трьох нових користувачів;
* створіть нову групу користувачів, туди додайте двох, з трьох створених користувачів;
* створіть новий файл, який буде доступний на зчитування, редагування та виконання власником файлу, наприклад найпростіший скриптовий сценарій;
* для користувачів групи власника надайте дозволи на перегляд та виконання (без дозволу на редагування) цього файлу;
* для інших користувачів заборонити доступ до цього файлу;



* \*подібні дії виконайте для директорій - створіть директорію, яка буде доступна для всіх трьох користувачів, створіть директорію, яку буде доступна тільки для власника, створіть директорію, яку користувачі групи власника зможуть переглядати, але не редагувати;

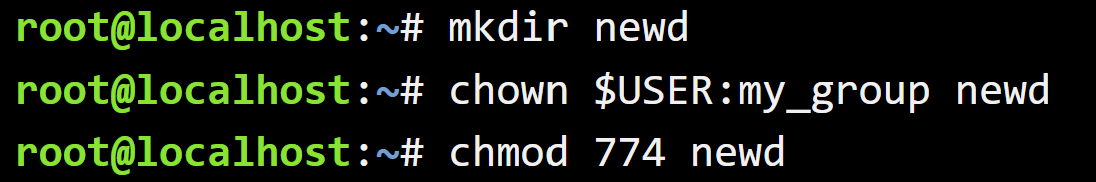


* \*створіть порожній файл під назвою emptyfile за допомогою команди touch emptyfile. Тепер “обнуліть” дозволи для файлу з chmod 000 emptyfile. Що станеться, якщо змінити дозволи для emptyfile, передавши лише одне значення для chmod у числовому режимі, наприклад, chmod 4 emptyfile? Що буде, якщо ми використаємо два числа, наприклад chmod 44 emptyfile? Що ми можемо дізнатися про те, як chmod зчитує числове значення?

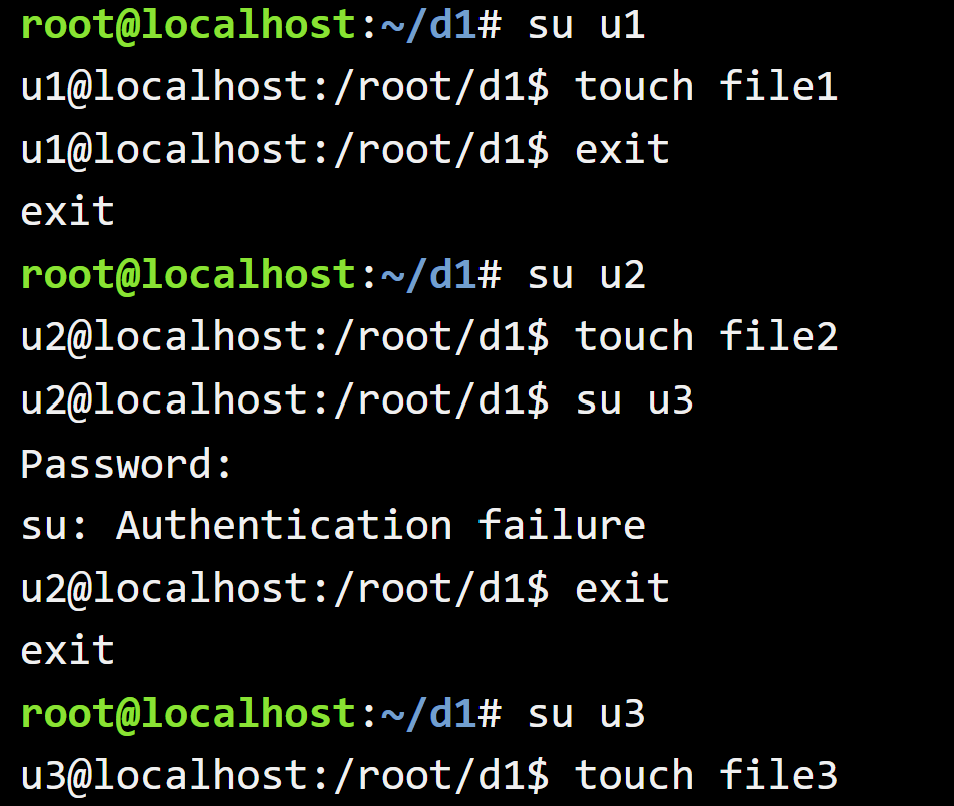


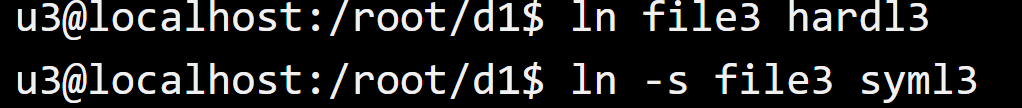
If you run chmod 4 emptyfile, only the owner will have read access to the file. If you run chmod 44 emptyfile, the owner and the group will have read permission to the file. The chmod command reads a numeric value as an octal number, where each digit corresponds to the permissions for the owner, group, and other users, respectively.

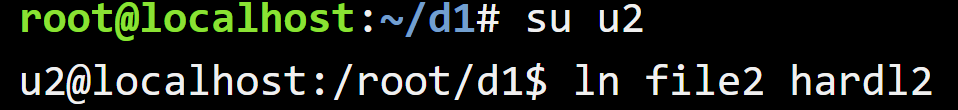
* \*\*створіть каталог під назвою, де всі файли автоматично будуть належати Вашій групі користувачів і можуть бути видалені лише користувачем, який їх створив?

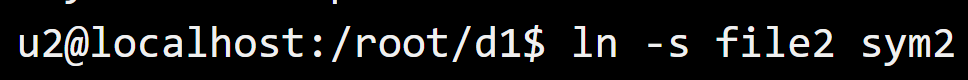


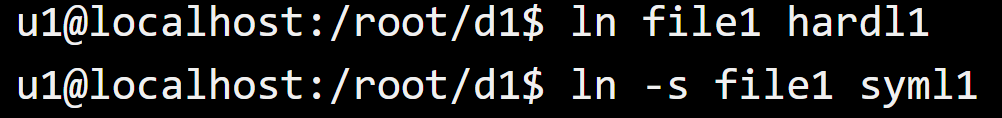
* \*\*під кожним користувачем створіть по одному новому файлу, та жорстке та символічне посилання на нього;









****

* \*\*спробуйте іншими користувачами переглянути ці файли;



* \*\*спробуйте іншими користувачами видалити ці файли, зробіть висновки.

rm /root/d1/u2/file2 (Термінал зависнув)

**Контрольні запитання:**

1. Наведіть приклади зміни прав доступу символічним методом (Symbolic Method)?

The symbolic method of changing access rights uses symbols to indicate the owner (u), group (g), others (o), or all (a), as well as the type of permission (read - r, write - w, execute - x). For example:

chmod u+x myfile – adds execute permission for the owner of the file.

chmod g-w myfile – removes write permission for a group.

1. Наведіть приклади зміни прав доступу числовим методом (numeric method, octal method)?

The numeric (octal) method of changing access rights uses numbers to set permissions. Each number corresponds to permissions for the owner, group, and others, respectively. For example:

chmod 700 myfile – sets full permissions for the owner, but no permissions for the group or others.

chmod 640 myfile – sets read and write permissions for the owner, read permissions for the group, but no permissions for others.

1. Яке призначення команди umask?

The umask command is used to set the default file creation mask value. This mask determines what permissions are not granted to new files and directories that are created.

1. Порівняйте жорсткі та символічні посилання?

A hard link is an additional name for an existing file on Linux or Unix. All hard links to a file point to the same storage location as the file itself. They are effectively the same file; deleting one of them will not affect the others.

A symbolic link (or soft link) is a separate file that points to another file or directory. It is analogous to a shortcut in Windows. Symbolic links can point to a file or directory that is on a different disk or partition. They can also point to files or directories that do not currently exist (these are called “dead links”).

1. \*Чи можна виконати файл, для якого є права на виконання, але не встановлені права на читання (--x)? Поясніть.

If you have the file's execute (--x) but not read (-r--) permissions, you can still execute the file. However, you will not be able to read the contents of the file with a command such as cat.

1. \*Якщо ми змінюємо права доступу та дозволи в поточній сесії чи будуть вони збережені в наступній?

Yes, if you change access rights or permissions for a file or directory, these changes will be saved and remain valid in subsequent sessions.

1. \*Чи є якийсь шаблон, яким система користується щодо прав та доступів при створенні нових файлів. Як можна змінити права дозволу за замовчуванням?

The default access rights template is defined using the umask command.

1. \*Яким чином можна створити жорстке посилання? В яких ситуаціях їх доцільно використовувати?

A hard link can be created using the ln command.

1. \*Яким чином можна створити символічне посилання? В яких ситуаціях їх доцільно використовувати?

You can create a symbolic link (or soft link) with the ln -s command. Symbolic links are useful when you need to create a link to a directory or when the original file may be moved or deleted. They point to the path of the original file, so if the original file is moved or deleted, the symbolic link will be “broken”.

1. \*\*Уявіть, що програмі потрібно створити одноразовий тимчасовий файл, який більше ніколи не знадобиться після закриття програми. Який правильний каталог для створення цього файлу?

The /tmp directory is usually used to create temporary files that are not needed after the program is closed. This directory is used to store temporary files that can be deleted without warning. The operating system can automatically clean up this directory during a reboot.

1. \*\*Є файл оригінал та для нього створено два посилання - символічне та жорстке. Що відбудеться з іншими файлами, якщо видалити:

* файл оригінал;

A hard link continues to point to the file data, so it is still accessible. A symbolic link, however, points to the file name, so it becomes “broken” or invalid.

* символічне посилання;

This does not affect the original file or hard link. They remain unchanged.

* жорстке посилання.

A file will be kept as long as there is at least one hard link to it. When the last hard link to a file is deleted, the file is also deleted.

**Висновки**

В ході виконання лабораторної роботи мною було досліджено тему зміни власників та прав доступу до файлів в Linux, більш детально теоретично досліджено питання спеціальних файлів і каталогів у Linux. Отримано практичні навички роботи з командами для визначення прав доступу до файлів у терміналі.